The secUnity Roadmap

5th France-Japan Cybersecurity Workshop

secUnity
supporting the security community

Sven Maier,
Karlsruhe Institute of Technology (KIT),
KASTEL

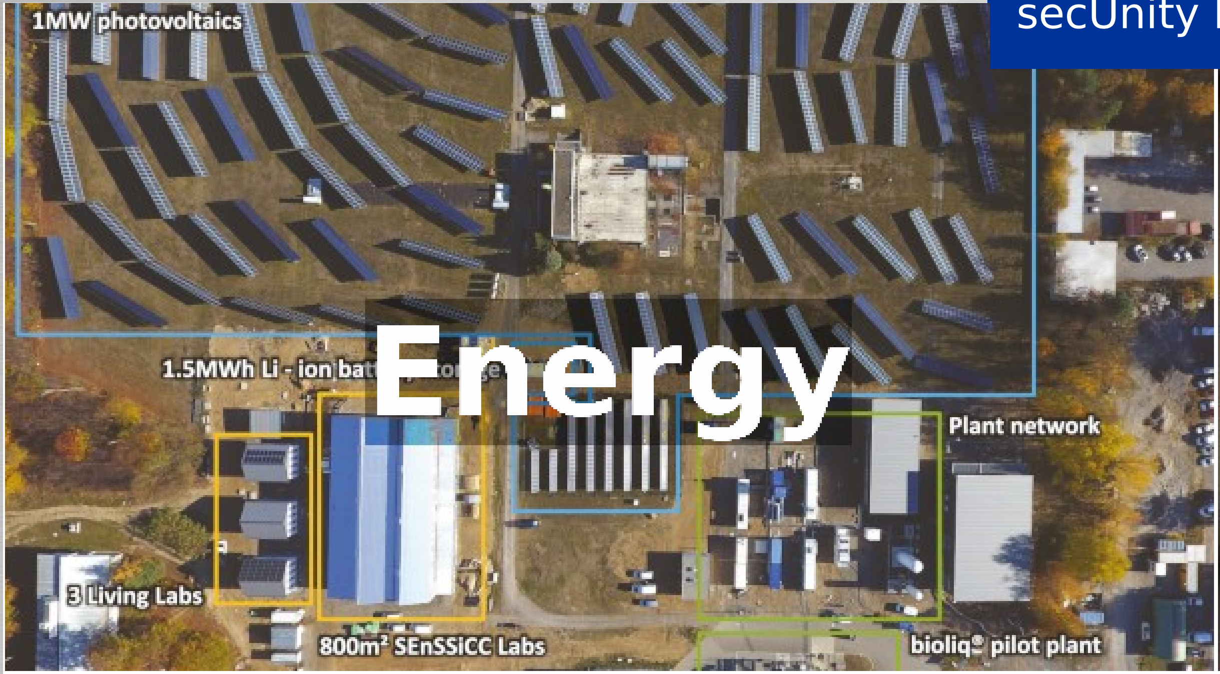
KASTEL

SPONSORED BY THE
Federal Ministry of Education and Research

KASTEL

- **Application Driven**
  - Comprehensive security for specific application areas.
- **Interdisciplinary**
  - Researchers from different fields:
    Cryptographers, IT security specialists, software-engineers, network security experts, jurists, economics, social scientists, …
- **Ambitious Goal: Quantifiable Security**
  - One of the great challenges of modern IT security and cryptography

secUnity Roadmap



SPONSORED BY THE
Federal Ministry
of Education
and Research

IT-security-map.eu

SPONSORED BY THE
Federal Ministry of Education and Research

Research Funding in Germany

KIT Karlsruhe Institute of Technology

Fraunhofer

RUHR UNIVERSITÄT BOCHUM RUB

TECHNISCHE UNIVERSITÄT DARMSTADT

DFG

HELMHOLTZ
RESEARCH FOR GRAND CHALLENGES

...

secUnity Roadmap

secUnity

SPONSORED BY THE

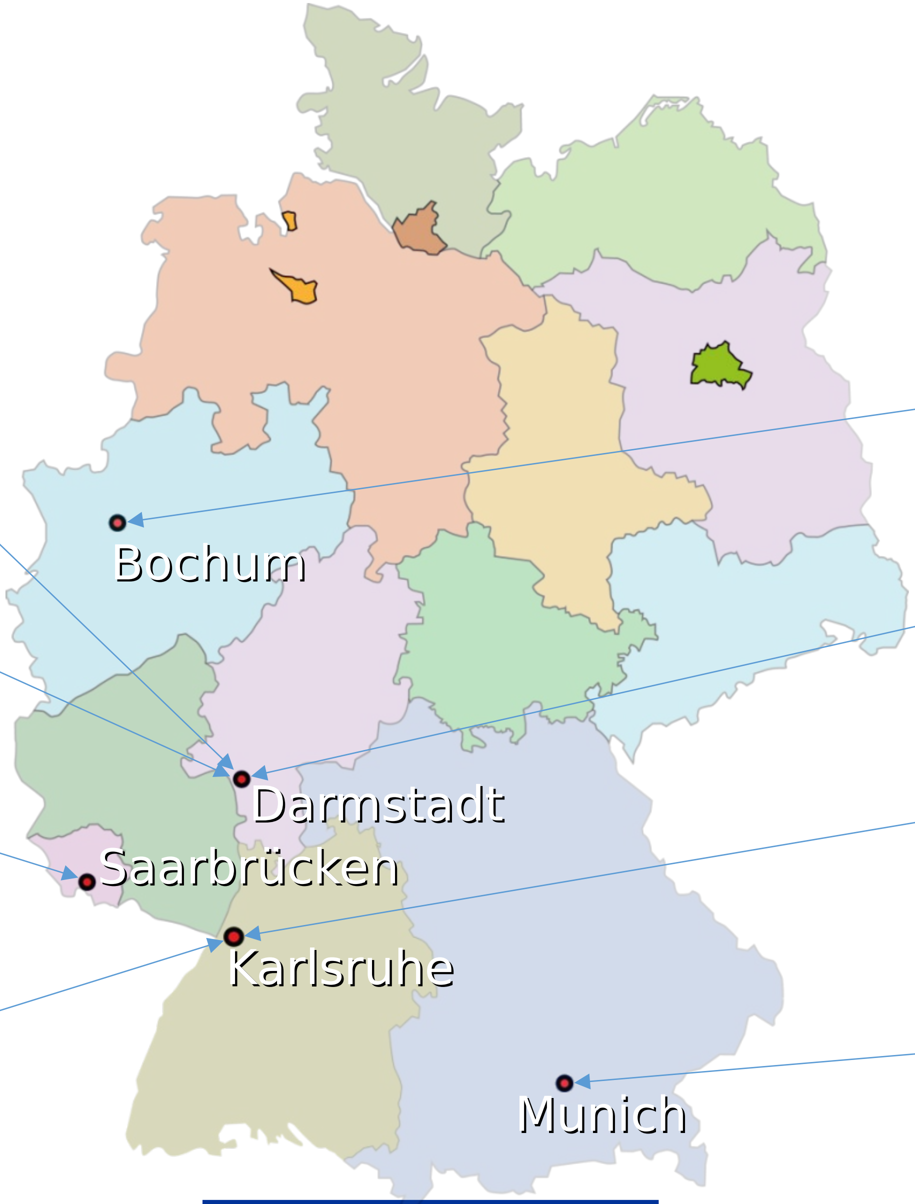
Federal Ministry of Education and Research

CRISP
Center for Research in Security and Privacy

TECHNISCHE UNIVERSITÄT DARMSTADT

CISPA
Center for IT-Security, Privacy and Accountability

KASTEL



RUHR UNIVERSITÄT BOCHUM
RUB

Fraunhofer
SIT

KIT
Karlsruhe Institute of Technology

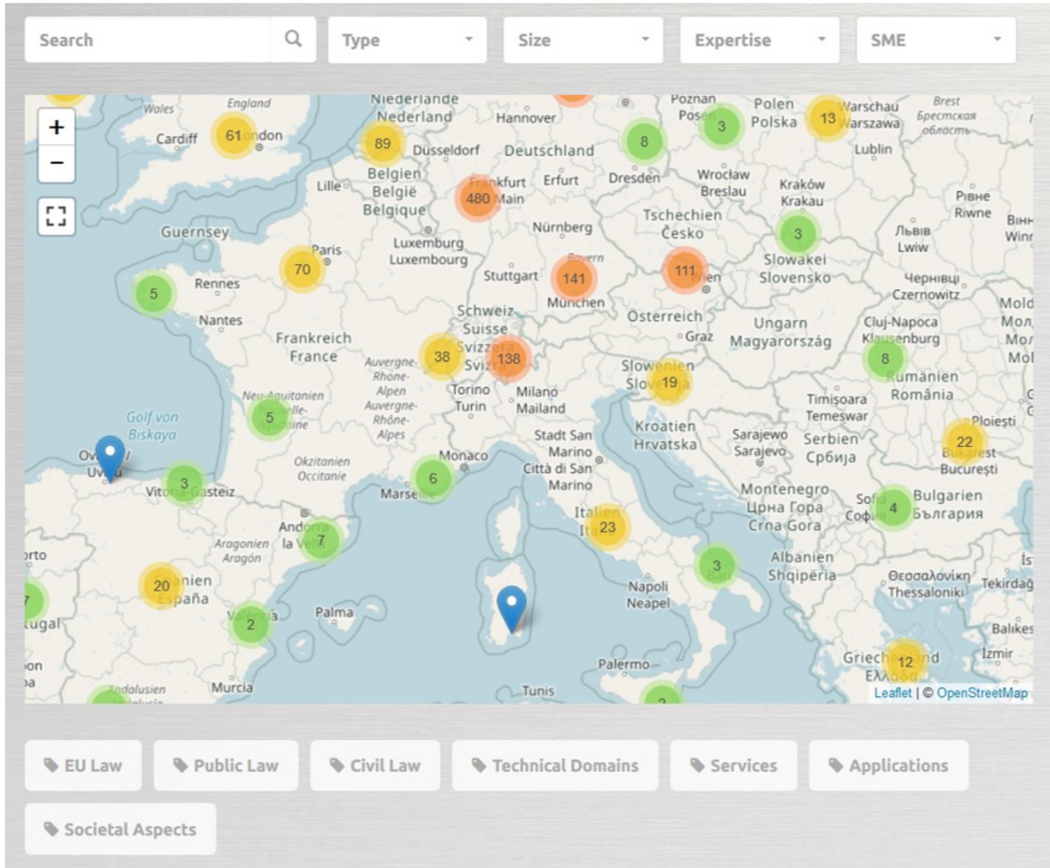
Fraunhofer
AISEC

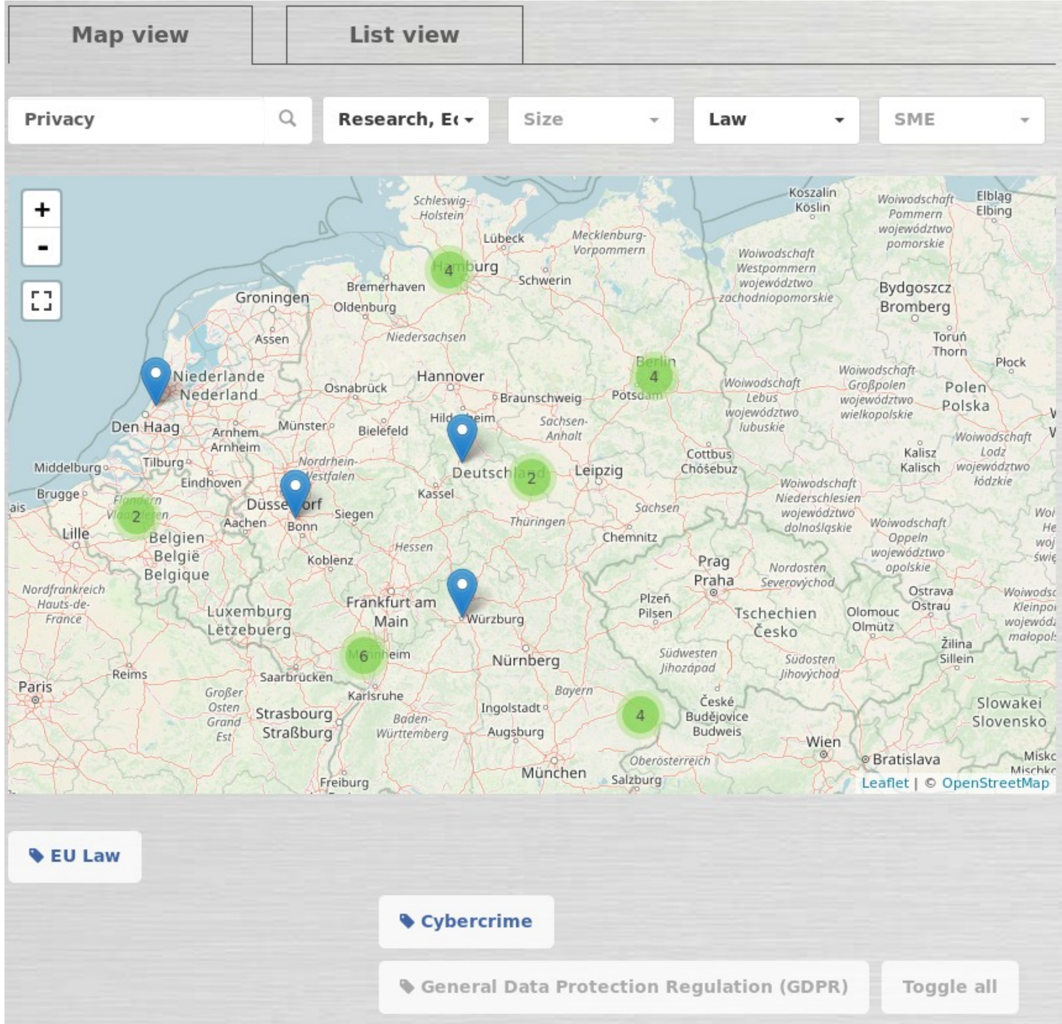
IT-security-map.eu

SPONSORED BY THE
Federal Ministry of Education and Research

secUnity: IT Security Map

- More than 1.700 entities





IT-security-map.eu

SPONSORED BY THE
Federal Ministry of Education and Research

secUnity-Roadmap

Cybersecurity Research: Challenges and Course of Action

Target Groups:

- Political Stakeholders
- Industry and Academia

Release:
5th of February 2019 in Brussels

Image © Eric Berghen

SPONSORED BY THE

Federal Ministry of Education and Research

Content

A. Key Challenges

1. Securing Cryptographic Systems against Emerging Attacks
2. Trustworthy Platforms
3. Secure Lifecycle Despite of Less Trustworthy Components
4. Quantifying Security
5. IT Security and Data Protection for Machine Learning
6. Big Data Privacy

B. Interdisciplinary Challenges

7. Measurable, Risk-adequate Security in Law
8. Holistic Human-centred Security and Privacy Research
9. Digital Business Models for a Fair Economy and Society

C. Technologies and Applications

1. Safeguarding Key Services of the Internet
2. Security of Blockchain Technology
3. Accountability and Transparency for Information Quality
4. User-centric privacy tools
5. Remotely Un-hackable PC
6. IT Security for Autonomous Driving

Online:

https://it-security-map.eu/en/roadmap/

SPONSORED BY THE

Federal Ministry of Education and Research

A1. Securing Cryptographic Systems against Emerging Attacks

- Problem: variety of brute-force and physical attacks on critical applications
- Required: transition to PQC (hybrid systems) and implement PQC secure against side-channel, fault or invasive attacks
- Required: research on „crypto-agile“ systems, i.a. flexible platforms, generic cryptographic accelerators
- Problem: new attacks with a) machine learning and b) on computer architecture (Spectre…)
- Required: new paradigm for „Making the common case fast“

SPONSORED BY THE
Federal Ministry of Education and Research

A1. Course of Action

Short-term	• Development of post-quantum algorithms, mitigation techniques for cache-timing and other implementation attacks • Design of resilient computer architectures
Mid-term	• Standardization and Dissemination of post-quantum algorithms • Implementation of the resilient architectures
Long-term	• Commercial spread of the resilient architectures

SPONSORED BY THE
Federal Ministry of Education and Research

A4. Quantifying Security

- Current situation: only heuristics available to judge a system's security
- Required: development of security metrics to
  - Compare the security of two system versions (e.g. before and after a patch)
  - Compare the benefit of different security measures (prioritisation)
- Difficult Problem! No single number will quantify security of a system.
- Required: combination of measures from different areas of cybersecurity
  - Furthering improved scientific rigour and a common language
  - Combining logical, deductive approach and the empirical, deductive one
  - Clarifying what aspects cannot be quantified

"Security" will never mean immunity against all attacks! …

SPONSORED BY THE
Federal Ministry of Education and Research

A4. Course of Action

Short-term	• Develop ways to compare different versions of the same system in terms of security • Compare advantages and limitations of different ways to quantify security • Identify aspects of security that cannot be quantified
Mid-term	• Develop a common language to talk about security quantification • Identify sensible ways to quantify security in sub-fields of IT security • Identify trade-offs between security measures • Develop security metrics adapted to specific application areas
Long-term	• Achieve security quantification of complex example systems • Quantify security of real systems

SPONSORED BY THE
Federal Ministry of Education and Research

A6. Big Data Privacy

- Problems: microtargeting, re-identification, revealing sensitive data, linkability
- **Anonymisation and Private Learning in Big Data:**
  - Adapt anonymisation methods to Big Data, i.e. address volume, velocity, and variety
  - Enhance privacy, e.g., Private Learning, Private Modelling or synthetic data
- **Expanding Cryptographic Schemes for Secure Computation:**
  - Improve scalability and adapt methods such as MPC, data anonymisation, and computation on encrypted data to Big Data
- **Standard Procedures for Efficient Privacy-Preserving Analytics:**
  - Develop holistic approach for handling personalised, sensitive Big Data
  - Include all processes, hardware and software, and networks for recording, storing, transferring, processing, and outputting data to guarantee protection of privacy
  - Auditable security

SPONSORED BY THE
Federal Ministry
of Education
and Research

A6. Course of Action

Short-term	• Extending and adapting (…) k-anonymity, l-diversity, t-closeness and Differential Privacy for Big Data • Use of trustworthy hardware security modules (… and) trusted initializer during preprocessing phase (…) • Implementation of MPC, secure against passive adversaries • Standards for isolated computers in data centres (auditable security)
Mid-term	• Development of new anonymization methods • Better insight and metrics of linkability, inference and re-identification risks • Development of efficient MPC secure against active adversaries • Efficient and feasible secure computation on encrypted data and efficient specialised protocols (…) • Comprehensive database for efficient PPA solutions
Long-term	• Private Learning and Private Modelling in order to allow value added without privacy risks • Implementation of efficient MPC, secure against active adversaries • (…) fully homomorphic encryption and usable indistinguishability obfuscation • Establishing a standard procedure efficient PPA with suitable privacy measure

SPONSORED BY THE
Federal Ministry of Education and Research

B2. Holistic Human-centred Security and Privacy Research

- Problem: Gap between theoretical and actual security caused by unrealistic assumptions (e.g. assuming end users choose secure passwords)
- New focus on software developers, system designers and administrators (instead of end user)
- Required: Holistic and systematic approach for design of security/privacy critical systems (in contrast to traditional research)
- Methodological challenges: selection of probands and in-depth replication study

SPONSORED BY THE
Federal Ministry
of Education
and Research

C5. Remotely unhackable PC

- Required: Remotely unhackable PC for private use, i.e.
  - Rule interactions between different components by strict protocols
  - Focus on usability (during all development steps)
- Suggest development of RUPC - starting from trustworthy hardware security modules, to systematic program analysis, to office packages and common browsers …
- Extension to intelligent personal assistants, AI

SPONSORED BY THE
Federal Ministry
of Education
and Research

C5. Course of Action

Short-term	• Deployment of trustworthy hardware security modules, hardened kernel and operation system • Specification of usability requirements
Mid-term	• RUPC extended by common browser and office packages • Usability tests
Long-term	• Full-featured, user-friendly RUPC • AI-based usability, remotely un-hackable intelligent personal assistant

The secUnity Roadmap

SPONSORED BY THE
Federal Ministry of Education and Research

A. Key Challenges

1. Securing Cryptographic Systems against Emerging Attacks
2. Trustworthy Platforms
3. Secure Lifecycle Despite of Less Trustworthy Components
4. Quantifying Security
5. IT Security and Data Protection for Machine Learning
6. Big Data Privacy

B. Interdisciplinary Challenges

7. Measurable, Risk-adequate Security in Law
8. Holistic Human-centred Security and Privacy Research
9. Digital Business Models for a Fair Economy and Society

C. Technologies and Applications

1. Safeguarding Key Services of the Internet
2. Security of Blockchain Technology
3. Accountability and Transparency for Information Quality
4. User-centric privacy tools
5. Remotely Un-hackable PC
6. IT Security for Autonomous Driving

Online:

https://it-security-map.eu/en/roadmap/

The secUnity Roadmap

5th France-Japan Cybersecurity Workshop

secUnity
supporting the security community

Thank you!

KASTEL